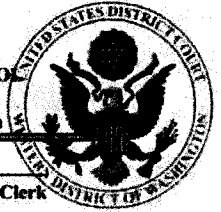


AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

CERTIFIED TRUE COPY
 ATTEST: WILLIAM M. MCCOOK
 Clerk, U.S. District Court
 Western District of Washington



By Emily New
 Deputy Clerk

UNITED STATES DISTRICT COURT

for the
 Western District of Washington

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)

18737 Fisherman's Loop, Burlington, WA 98233 (Subject
 Premises); James Sims (Subject Person)

Case No. MJ18-457

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Subject Premises and Subject Person as further described in Attachment A, which is attached hereto and incorporated herein by this reference.
 located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography
Title 18, U.S.C. § 2251(a)(e)	Production of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Terry Getsch
 Applicant's signature

SPECIAL AGENT TERRY GETSCH, FBI
 Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone (specify reliable electronic means).

Date: 10/01/2018

City and state: BELLINGHAM, WASHINGTON

Paula L McCandlis
 Judge's signature

PAULA L. MCCANDLIS, U.S. MAGISTRATE JUDGE

Printed name and title 2018R01166

ATTACHMENT A

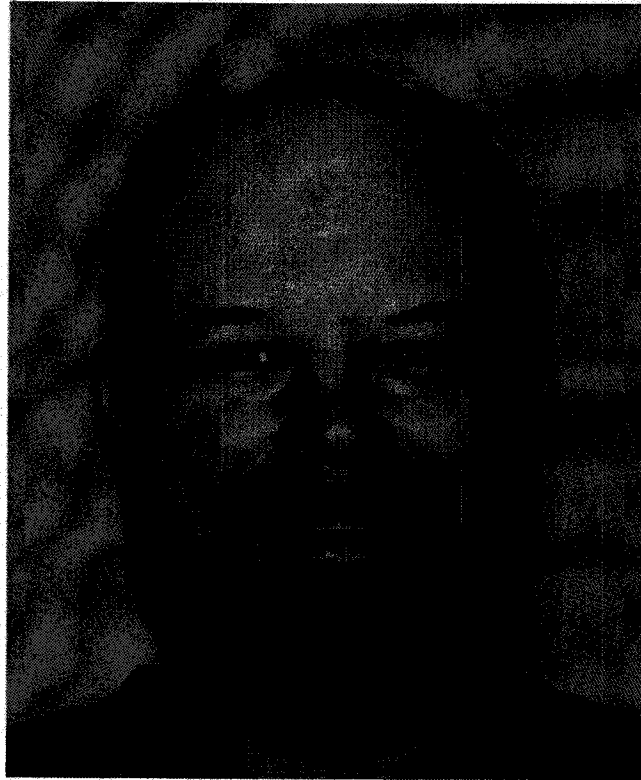
Description of Property to be Searched

1. The physical address of the SUBJECT PREMISES is 18737 Fisherman's Loop, Burlington, WA 98233. The SUBJECT PREMISES is the property at this address containing a single family, single story residence located in Skagit County, WA. The residence was previously identified by the Skagit County Tax assessor by the picture below:



The search is to include all rooms, persons, and vehicles on the SUBJECT PREMISES, as well as any garage/parking spaces or storage units/outbuildings located thereon and any digital device(s) found therein.

1 The SUBJECT PERSON is JAMES R. SIMS (DOB: XX/XX/1973), pictured
2 below:



ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence/records identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer, or evidences contact with minors;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

1 7. Digital devices and/or their components, which include, but are not limited
2 to:

3 a. Any digital devices and storage device capable of being used to
4 commit, further, or store evidence of the offense listed above;

5 b. Any digital devices used to facilitate the transmission, creation,
6 display, encoding or storage of data, including word processing equipment, modems,
7 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

8 c. Any magnetic, electronic, or optical storage device capable of
9 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
10 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
11 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

12 d. Any documentation, operating logs and reference manuals regarding
13 the operation of the digital device or software;

14 e. Any applications, utility programs, compilers, interpreters, and other
15 software used to facilitate direct or indirect communication with the computer hardware,
16 storage devices, or data to be searched;

17 f. Any physical keys, encryption devices, dongles and similar physical
18 items that are necessary to gain access to the computer equipment, storage devices or
19 data; and

20 g. Any passwords, password files, test keys, encryption codes or other
21 information necessary to access the computer equipment, storage devices or data;

22 8. Evidence of who used, owned or controlled any seized digital device(s) at
23 the time the things described in this warrant were created, edited, or deleted, such as logs,
24 registry entries, saved user names and passwords, documents, and browsing history;

25 9. Evidence of malware that would allow others to control any seized digital
26 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
27 as evidence of the presence or absence of security software designed to detect malware;
28 as well as evidence of the lack of such malware;

1 10. Evidence of the attachment to the digital device(s) of other storage devices
2 or similar containers for electronic evidence;

3 11. Evidence of counter-forensic programs (and associated data) that are
4 designed to eliminate data from a digital device;

5 12. Evidence of times the digital device(s) was used;

6 13. Any other ESI from the digital device(s) necessary to understand how the
7 digital device was used, the purpose of its use, who used it, and when.

8 14. Records and things evidencing the use of the IP addresses 172.92.195.206
9 (the SUBJECT IP ADDRESS) including:

10 a. Routers, modems, and network equipment used to connect
11 computers to the Internet;

12 b. Records of Internet Protocol (IP) addresses used;

13 c. Records of Internet activity, including firewall logs, caches, browser
14 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
15 entered into any Internet search engine, and records of user-typed web addresses.

16
17
18 **The seizure of digital devices and/or their components as set forth herein is**
19 **specifically authorized by this search warrant, not only to the extent that such**
20 **digital devices constitute instrumentalities of the criminal activity described above,**
21 **but also for the purpose of the conducting off-site examinations of their contents for**
22 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
23
24
25
26
27
28

AFFIDAVIT

STATE OF WASHINGTON)

) ss

COUNTY OF WHATCOM)

I, Terry Aaron Getsch, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I, Terry A. Getsch, being first duly sworn on oath, depose and say:

2. I, Terry A. Getsch, am a Special Agent (SA) of the Federal Bureau of Investigation (FBI), assigned to the Bellingham, Washington, Resident Agency of the Seattle, Washington, Field Office. I am a graduate of the FBI Academy in Quantico, Virginia, and I have been employed by the FBI as a Special Agent since July 2018. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I was previously employed for over three years as a Police Officer and Detective with the Richmond Hill Police Department (RHPD) in Georgia. In my time as a law enforcement officer, I have investigated cases involving the sexual abuse of minors.

3. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at 18737 Fisherman's Loop, Burlington, WA 98233 (hereinafter the "SUBJECT PREMISES") and the person of JAMES SIMS (the "SUBJECT PERSON"), as more fully described in Attachment A to this Affidavit, including any digital devices, for the things described in Attachment B to this Affidavit, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251 (Production of Child Pornography, 18

1 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. §
2 2252(a)(4)(B) (Possession of Child Pornography).

3 4. The facts set forth in this Affidavit are based on my own personal
4 knowledge; knowledge obtained from other individuals during my participation in this
5 investigation, including other law enforcement officers; review of documents and records
6 related to this investigation; communications with others who have personal knowledge
7 of the events and circumstances described herein; and information gained through my
8 training and experience. My descriptions of the images below are based on my
9 experience and conversations with other FBI Special Agents and subject matter experts.

10 5. Because this Affidavit is submitted for the limited purpose of establishing
11 probable cause in support of the application for a search warrant, it does not set forth
12 each and every fact that I or others have learned during the course of this investigation. I
13 have set forth only the facts that I believe are relevant to the determination of probable
14 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C.
15 § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or
16 Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child
17 Pornography), will be found at the SUBJECT PREMISES, or on the SUBJECT
18 PERSON.

19 6. This Affidavit is being presented electronically pursuant to Local Criminal
20 Rule CrR 41(d)(3).

21 II. STATEMENT OF PROBABLE CAUSE

22 7. Between September 25 and 27, 2018, I was notified of an ongoing
23 investigation involving the distribution, receipt, and possession of child pornography by
24 the FBI Child Exploitation Task Force in Salt Lake City, Utah. Investigators had utilized
25 a software program to record online activity, chats, and images/videos being exchanged
26 over the Kik messaging platform through an online covert employee (OCE) connected to
27 the Internet in an undercover capacity from a computer located at the FBI Office in Salt
28 Lake City, Utah.

1 8. The OCE had posted numerous online bulletin messages on specific social
 2 media forums, which, the OCE knew to be websites frequented by individuals who have
 3 a sexual interest in children and incest. The bulletin messages were intended to attract
 4 individuals with a sexual interest in children. The FBI OCE would respond to certain
 5 messages or post messages on these public forums and provided the OCE's KiK screen
 6 name. KiK refers KiK Messenger, a free mobile application that permits users to send
 7 text messages and other content, including videos and images.

8 9. Between September 25 and 28, 2018, the OCE was a member of a known
 9 child pornography group, where members of this KiK group would discuss sexually
 10 abusing children and post images/videos of child rape. An individual with the KiK
 11 profile name "kenworth105" and using the screen name "James S" (identified as and
 12 hereafter referred to as JAMES SIMS) was a member of this group. KiK user
 13 "kenworth105" commented about sexually abusing children and commented about other
 14 images of child pornography that were posted to the group. The FBI OCE posted an
 15 advertisement to the group claiming to have a fictitious nine-year-old daughter by
 16 sending a KiK message. KiK user "kenworth105" then began communicating with the
 17 OCE privately outside of the group. That user told the OCE he had been sexually
 18 abusing [REDACTED] since she was six. He also sent the OCE pictures
 19 that he claimed were of [REDACTED] (non-nude) and a close up view of a girl's
 20 genitals and chest, which he claimed to be of [REDACTED] This Kik user also sent
 21 images of prepubescent children engaged in sexual acts with adults and other children
 22 and asked the OCE to abuse his fictitious daughter and send him images of that abuse.
 23 The following reflect exmples of chats between the OCE and "kenworth105" (JAMES
 24 SIMS):

25 OCE: Hey what r u into? I'm a 38 yo dad with a 9 yo dau

26 JAMES SIMS: Hi

27 OCE: What r u into? Ages?

28 JAMES SIMS: 0-13 and mom

1 OCE: Hot ru active with anyone

2 JAMES SIMS: Rarely with [REDACTED] are you

3 OCE: Mmm yes I am, wish I was more, what have u done

4 JAMES SIMS: Who and what age

5 OCE: With my dau who is 9, what have u done with [REDACTED]

6 JAMES SIMS: Everything with [REDACTED] since she was 6

7 OCE: Everything? nice

8 JAMES SIMS: Yes, You

9 OCE: Mainly rubbing licking touching oral, working my way up, Is she still

10 [REDACTED]
11 JAMES SIMS: Mmmmm That makes me hard, Last time was a month ago

12 OCE: That sucks, u a truck driver probably makes it hard, I'm [REDACTED]

13 [REDACTED]
14 JAMES SIMS: Have a pic

15 OCE: Yes I'm open to sharing pics, what do u have?

16 JAMES SIMS: [Image sent depicting two nude prepubescent age children (boy
17 and girl) lying on a bed engaged in sexual acts]

18 OCE: Hot

19 JAMES SIMS: [Video sent depicting the vaginal rape of a nude toddler age
20 girl by an adult female using a sex toy]

21 ***

22 JAMES SIMS: [Image sent depicting a nude chest. This image is claimed by

23 JAMES SIMS to be [REDACTED]

24 JAMES SIMS: [Image sent depicting a close up view of female genital being
25 spread being spread apart. This image is claimed by JAMES SIMS to be of [REDACTED]

26 [REDACTED]
27 OCE: How old is she now?

28 JAMES SIMS: 14

1 OCE: For real? She looks older

2 JAMES SIMS: Yes

3 OCE: Nice, Do u ever drive thru Salt Lake City?

4 JAMES SIMS: [Image sent depicting JAMES SIMS and 

5 
6 OCE: Cute, how do u keep her quiet, that's always my worry

7 JAMES SIMS: Yes, it is her choice to play or not, Yes I have been to Salt
8 Lake City

9 OCE: Cool u r lucky and I'm jealous, u started when she was six? 

10 
11 JAMES SIMS: Yes, No

12 OCE: I live in Salt Lake City and looking for like minded dads

13 JAMES SIMS: Nice Washington State

14 OCE: Cool

15 JAMES SIMS: Yeah

16 OCE: Luv Incest

17 JAMES SIMS: Yes

18 OCE: R u active with anyone else

19 JAMES SIMS: No, I want a mom and kids

20 ***

21 JAMES SIMS: Love to see if you wanted to share

22 OCE: Hmm I'm open what did u have in mind?

23 JAMES SIMS: I always love pictures or videos, I can share what I have as
24 well

25 JAMES SIMS: [Image sent depicting JAMES SIMS and an adult female
26 (nonnude)]

27 ***

28 JAMES SIMS: [Image sent depicting the close up view of the anus and

1 vaginal area of what appears to be an infant/toddler being vaginally raped by an
2 adult male]

3 ***

4 JAMES SIMS: [Image sent depicting the close up view of the anus and
5 vaginal area of what looks to be a prepubescent girl]

6 10. On September 25, 2018, FBI Salt Lake City sent an administrative
7 subpoena to KiK requesting subscriber data for account user "kenworth105.". Kik
8 responded the next day with the following subscriber data:

9 First Name: James

10 Last Name: S

11 Email: peterdervie@me.com

12 Username: kenworth105

13 Registration Device: iPhone

14 IP Address: 172.92.195.206

15 11. According to Kik, the IP address listed above was among the IP addresses
16 used to access Kik account "kenworth105" on September 25 and 26, 2018.

17 12. On September 26, 2018, FBI Salt Lake City sent an administrative
18 subpoena to Wave Broadband requesting the subscriber information for IP address
19 172.92.195.206. That same day, Wave Broadband reported that this IP address was
20 assigned to the following subscriber on September 25, 2018:

21 Customer Name: Stacey Sims

22 Service Address: 18737 Fisherman's Loop, Burlington, WA 98233

23 Telephone Number: (XXX) XXX-5101, (XXX) XXX-7582

24 Length of Service: Account created 01/07/10

25 13. Database and social media searches for people connected to the KiK
26 account or connected to the address found include the following:

27 Name: James Robert Sims
28

1 Race: White

2 Sex: Male

3 DOB: XX/XX/1973

4 SSN: XXX-XX-4984, XXX-XX-4486

5 Address: 18737 Fisherman's Loop, Burlington, WA 98233

6 Criminal History: Domestic Violence (non-conviction)

7 Possible Employment: Truck Driver

8 14. I have reviewed James Robert Sims's criminal history and identified that he
9 has one misdemeanor conviction for Resisting Arrest in Sedro Wooley, Washington from
10 1994.

11 15. I conducted a review of the Washington State Weapons/Permit Registration
12 database and learned that James Sims purchased a Sig-Sauer Pistol (Serial Number:
13 AKU16115) in Washington state on March 3, 2017, and obtained a Concealed Pistol
14 License on November 10, 2016.

15 16. I have reviewed James Robert Sims's Washington Department of Licensing
16 information, and identified a listed address of 18737 Fisherman's Loop, Burlington, WA
17 98233 (the SUBJECT PREMISES) for James Robert Sims's Washington driver license.

18 17. On October 1 2018, I received an original copy of the recorded KiK
19 messenger conversations between the OCE and Kik user "kenworth105," as well as
20 images and videos sent by "kenworth105" to the OCE referenced above. I reviewed these
21 images and describe several below:

- 22 • Kik user "Kenworth105" sent a video that is one minute and fifty-six
23 seconds long that depicts an adult female using a dildo to vaginally
24 penetrate a female toddler. The child has no pubic hair, is small in stature
25 in comparison to the adult female, and lacks muscular and breast
26 development. I estimate she is under the age of five.

- Kik user "Kenworth105" sent an image depicting a prepubescent boy and a prepubescent girl. Both are nude, and the girl has her hand on the boy's erect penis. Both are small in stature, lack pubic hair and development, are youthful in appearance, and lack muscular development. I estimate both children are between the ages of five to nine.
- Kik user "kenworth105" sent an image of an adult male and [REDACTED]. As noted above, that user identified this as a picture of himself and [REDACTED]. The adult male matches the Washington DOL photo for JAMES SIMS. And the [REDACTED] of [REDACTED].

III. PRIOR EFFORTS TO OBTAIN EVIDENCE

18. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview with JAMES SIMS, or any other unknown resident(s) or occupant(s) of the SUBJECT PREMISES, they could rightfully refuse to give consent and the user who distributed child pornography files as outlined above could arrange for destruction of all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT PREMISES or the SUBJECT PERSON.

IV. TECHNICAL BACKGROUND

19. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet, the individual's IP address is visible to administrators of websites they visit. Further, the

1 individual's IP address is broadcast during most Internet file and information exchanges
2 that occur.

3 20. Based on my training and experience, I know that most ISPs provide only
4 one IP address for each residential subscription. I also know that individuals often use
5 multiple digital devices within their home to access the Internet, including desktop and
6 laptop computers, tablets, and mobile phones. A device called a router is used to connect
7 multiple digital devices to the Internet via the public IP address assigned (to the
8 subscriber) by the ISP. A wireless router performs the functions of a router but also
9 includes the functions of a wireless access point, allowing (wireless equipped) digital
10 devices to connect to the Internet via radio waves, not cables. Based on my training and
11 experience, today many residential Internet customers use a wireless router to create a
12 computer network within their homes where users can simultaneously access the Internet
13 (with the same public IP address) with multiple digital devices.

14 21. Based on my training and experience and information provided to me by
15 computer forensic agents, I know that data can quickly and easily be transferred from one
16 digital device to another digital device. Data can be transferred from computers or other
17 digital devices to internal and/or external hard drives, tablets, mobile phones, and other
18 mobile devices via a USB cable or other wired connection. Data can also be transferred
19 between computers and digital devices by copying data to small, portable data storage
20 devices including USB (often referred to as "thumb") drives, memory cards (Compact
21 Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

22 22. As outlined above, residential Internet users can simultaneously access the
23 Internet in their homes with multiple digital devices. Also explained above is how data
24 can quickly and easily be transferred from one digital device to another through the use
25 of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage
26 devices (USB drives, memory cards, optical discs). Therefore, a user could access the
27 Internet using their assigned public IP address, receive, transfer or download data, and
28

1 then transfer that data to other digital devices, which may or may not have been
2 connected to the Internet during the date and time of the specified transaction.

3 23. Based on my training and experience, I have learned that the computer's
4 ability to store images and videos in digital form makes the computer itself an ideal
5 repository for child pornography. The size of hard drives used in computers (and other
6 digital devices) has grown tremendously within the last several years. Hard drives with
7 the capacity of four (4) terabytes (TB) are not uncommon. These drives can store
8 thousands of images and videos at very high resolution.

9 24. Based on my training and experience, and information provided to me by
10 other law enforcement officers, I know that people tend to use the same user names
11 across multiple accounts and email services.

12 25. Based on my training and experience, collectors and distributors of child
13 pornography also use online resources to retrieve and store child pornography, including
14 services offered by companies such as Google, Yahoo, Apple, and Dropbox, among
15 others. The online services allow a user to set up an account with a remote computing
16 service that provides email services and/or electronic storage of computer files in any
17 variety of formats. A user can set up an online storage account from any computer with
18 access to the Internet. Evidence of such online storage of child pornography is often
19 found on the user's computer. Even in cases where online storage is used, however,
20 evidence of child pornography can be found on the user's computer in most cases.

21 26. As is the case with most digital technology, communications by way of
22 computer can be saved or stored on the computer used for these purposes. Storing this
23 information can be intentional, i.e., by saving an email as a file on the computer or saving
24 the location of one's favorite websites in, for example, "bookmarked" files. Digital
25 information can also be retained unintentionally, e.g., traces of the path of an electronic
26 communication may be automatically stored in many places (e.g., temporary files or ISP
27 client software, among others). In addition to electronic communications, a computer
28 user's Internet activities generally leave traces or "footprints" and history files of the

1 browser application used. A forensic examiner often can recover evidence suggesting
2 whether a computer contains wireless software, and when certain files under investigation
3 were uploaded or downloaded. Such information is often maintained indefinitely until
4 overwritten by other data.

5 27. Based on my training and experience, I have learned that producers of child
6 pornography can produce image and video digital files from the average digital camera,
7 mobile phone, or tablet. These files can then be easily transferred from the mobile device
8 to a computer or other digital device, using the various methods described above. The
9 digital files can then be stored, manipulated, transferred, or printed directly from a
10 computer or other digital device. Digital files can also be edited in ways similar to those
11 by which a photograph may be altered; they can be lightened, darkened, cropped, or
12 otherwise manipulated. As a result of this technology, it is relatively inexpensive and
13 technically easy to produce, store, and distribute child pornography. In addition, there is
14 an added benefit to the child pornographer in that this method of production is a difficult
15 trail for law enforcement to follow.

16 28. As part of my training and experience, I have become familiar with the
17 structure of the Internet, and I know that connections between computers on the Internet
18 routinely cross state and international borders, even when the computers communicating
19 with each other are in the same state. Individuals and entities use the Internet to gain
20 access to a wide variety of information; to send information to, and receive information
21 from, other individuals; to conduct commercial transactions; and to communicate via
22 email.

23 29. Based on my training and experience, I know that cellular mobile phones
24 (often referred to as "smart phones") have the capability to access the Internet and store
25 information, such as images and videos. As a result, an individual using a smart phone
26 can send, receive, and store files, including child pornography, without accessing a
27 personal computer or laptop. An individual using a smart phone can also easily connect
28 the device to a computer or other digital device, via a USB or similar cable, and transfer

1 data files from one digital device to another. Moreover, many media storage devices,
2 including smartphones and thumb drives, can easily be concealed and carried on an
3 individual's person and smartphones and/or mobile phones are also often carried on an
4 individual's person.

5 30. As set forth herein and in Attachment B to this Affidavit, I seek permission
6 to search for and seize evidence, fruits, and instrumentalities of the above-referenced
7 crimes that might be found at the SUBJECT PREMISES or on the SUBJECT PERSON,
8 in whatever form they are found. It has been my experience that individuals involved in
9 child pornography often prefer to store images of child pornography in electronic form.
10 The ability to store images of child pornography in electronic form makes digital devices,
11 examples of which are enumerated in Attachment B to this Affidavit, an ideal repository
12 for child pornography because the images can be easily sent or received over the Internet.
13 As a result, one form in which these items may be found is as electronic evidence stored
14 on a digital device.

15 31. Based upon my knowledge, experience, and training in child pornography
16 investigations, and the training and experience of other law enforcement officers with
17 whom I have had discussions, I know that there are certain characteristics common to
18 individuals who have a sexualized interest in children and depictions of children:

19 a. They may receive sexual gratification, stimulation, and satisfaction
20 from contact with children; or from fantasies they may have viewing children engaged in
21 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
22 visual media; or from literature describing such activity.

23 b. They may collect sexually explicit or suggestive materials in a
24 variety of media, including photographs, magazines, motion pictures, videotapes, books,
25 slides, and/or drawings or other visual media. Such individuals often times use these
26 materials for their own sexual arousal and gratification. Further, they may use these
27 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
28 selected child partner, or to demonstrate the desired sexual acts. These individuals may

1 keep records, to include names, contact information, and/or dates of these interactions, of
2 the children they have attempted to seduce, arouse, or with whom they have engaged in
3 the desired sexual acts.

4 c. They often maintain any "hard copies" of child pornographic
5 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
6 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
7 their home or some other secure location. These individuals typically retain these "hard
8 copies" of child pornographic material for many years, as they are highly valued.

9 d. Likewise, they often maintain their child pornography collections
10 that are in a digital or electronic format in a safe, secure and private environment, such as
11 a computer and surrounding area. These collections are often maintained for several
12 years and are kept close by, often at the individual's residence or some otherwise easily
13 accessible location, to enable the owner to view the collection, which is valued highly.

14 e. They also may correspond with and/or meet others to share
15 information and materials; rarely destroy correspondence from other child pornography
16 distributors/collectors; conceal such correspondence as they do their sexually explicit
17 material; and often maintain lists of names, addresses, and telephone numbers of
18 individuals with whom they have been in contact and who share the same interests in
19 child pornography.

20 f. They generally prefer not to be without their child pornography for
21 any prolonged time period. This behavior has been documented by law enforcement
22 officers involved in the investigation of child pornography throughout the world.

23 g. E-mail itself provides a convenient means by which individuals can
24 access a collection of child pornography from any computer, at any location with Internet
25 access. Such individuals therefore do not need to physically carry their collections with
26 them but rather can access them electronically. Furthermore, these collections can be
27 stored on email "cloud" servers, which allow users to store a large amount of material at
28 no cost, without leaving any physical evidence on the users' computer(s).

1 32. In addition to offenders who collect and store child pornography, law
2 enforcement has encountered offenders who obtain child pornography from the internet,
3 view the contents and subsequently delete the contraband, often after engaging in self-
4 gratification. In light of technological advancements, increasing Internet speeds and
5 worldwide availability of child sexual exploitative material, this phenomenon offers the
6 offender a sense of decreasing risk of being identified and/or apprehended with quantities
7 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
8 offender, knowing that the same or different contraband satisfying their interests remain
9 easily discoverable and accessible online for future viewing and self-gratification. I
10 know that, regardless of whether a person discards or collects child pornography he/she
11 accesses for purposes of viewing and sexual gratification, evidence of such activity is
12 likely to be found on computers and related digital devices, including storage media, used
13 by the person. This evidence may include the files themselves, logs of account access
14 events, contact lists of others engaged in trafficking of child pornography, backup files,
15 and other electronic artifacts that may be forensically recoverable.

16 33. Given the above-stated facts, and based on my knowledge, training and
17 experience, along with my discussions with other law enforcement officers who
18 investigate child exploitation crimes, I believe that the user "kenworth105" likely has a
19 sexualized interest in children and depictions of children and that evidence of child
20 pornography is likely to be found on digital media devices, including mobile and/or
21 portable digital devices that belong to this user or to which this user has access.

22 34. Based on my training and experience, and that of computer forensic agents
23 that I work and collaborate with on a daily basis, I know that every type and kind of
24 information, data, record, sound or image can exist and be present as electronically stored
25 information on any of a variety of computers, computer systems, digital devices, and
26 other electronic storage media. I also know that electronic evidence can be moved easily
27 from one digital device to another. As a result, I believe that electronic evidence may be
28

1 stored on any digital device present at the SUBJECT PREMISES or on the SUBJECT
2 PERSON.

3 35. Based on my training and experience, and my consultation with computer
4 forensic agents who are familiar with searches of computers, I know that in some cases
5 the items set forth in Attachment B may take the form of files, documents, and other data
6 that is user-generated and found on a digital device. In other cases, these items may take
7 the form of other types of data - including in some cases data generated automatically by
8 the devices themselves.

9 36. Based on my training and experience, and my consultation with computer
10 forensic agents who are familiar with searches of computers, I believe that if digital
11 devices are found in the SUBJECT PREMISES or on the SUBJECT PERSON, there is
12 probable cause to believe that the items set forth in Attachment B will be stored in those
13 digital devices for a number of reasons, including but not limited to the following:

14 a. Once created, electronically stored information (ESI) can be stored
15 for years in very little space and at little or no cost. A great deal of ESI is created, and
16 stored, moreover, even without a conscious act on the part of the device operator. For
17 example, files that have been viewed via the Internet are sometimes automatically
18 downloaded into a temporary Internet directory or "cache," without the knowledge of the
19 device user. The browser often maintains a fixed amount of hard drive space devoted to
20 these files, and the files are only overwritten as they are replaced with more recently
21 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
22 include relevant and significant evidence regarding criminal activities, but also, and just
23 as importantly, may include evidence of the identity of the device user, and when and
24 how the device was used. Most often, some affirmative action is necessary to delete ESI.
25 And even when such action has been deliberately taken, ESI can often be recovered,
26 months or even years later, using forensic tools.

27 b. Wholly apart from data created directly (or indirectly) by user-
28 generated files, digital devices - in particular, a computer's internal hard drive - contain

1 electronic evidence of how a digital device has been used, what it has been used for, and
2 who has used it. This evidence can take the form of operating system configurations,
3 artifacts from operating systems or application operations, file system data structures, and
4 virtual memory "swap" or paging files. Computer users typically do not erase or delete
5 this evidence, because special software is typically required for that task. However, it is
6 technically possible for a user to use such specialized software to delete this type of
7 information - and, the use of such special software may itself result in ESI that is relevant
8 to the criminal investigation. In particular, to properly retrieve and analyze electronically
9 stored (computer) data, and to ensure accuracy and completeness of such data and to
10 prevent loss of the data either from accidental or programmed destruction, it is necessary
11 to conduct a forensic examination of the computers. To effect such accuracy and
12 completeness, it may also be necessary to analyze not only data storage devices, but also
13 peripheral devices which may be interdependent, the software to operate them, and
14 related instruction manuals containing directions concerning operation of the computer
15 and software.

16 **V. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

17 37. In addition, based on my training and experience and that of computer
18 forensic agents that I work and collaborate with on a daily basis, I know that in most
19 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
20 electronic evidence stored on a digital device during the physical search of a search site
21 for a number of reasons, including but not limited to the following:

22 a. Technical Requirements: Searching digital devices for criminal
23 evidence is a highly technical process requiring specific expertise and a properly
24 controlled environment. The vast array of digital hardware and software available
25 requires even digital experts to specialize in particular systems and applications, so it is
26 difficult to know before a search which expert is qualified to analyze the particular
27 system(s) and electronic evidence found at a search site. As a result, it is not always
28 possible to bring to the search site all of the necessary personnel, technical manuals, and

1 specialized equipment to conduct a thorough search of every possible digital
2 device/system present. In addition, electronic evidence search protocols are exacting
3 scientific procedures designed to protect the integrity of the evidence and to recover even
4 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is
5 extremely vulnerable to inadvertent or intentional modification or destruction (both from
6 external sources and from destructive code embedded in the system such as a "booby
7 trap"), a controlled environment is often essential to ensure its complete and accurate
8 analysis.

9 b. Volume of Evidence: The volume of data stored on many digital
10 devices is typically so large that it is impossible to search for criminal evidence in a
11 reasonable period of time during the execution of the physical search of a search site. A
12 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A
13 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000
14 double-spaced pages of text. Computer hard drives are now being sold for personal
15 computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally,
16 this data may be stored in a variety of formats or may be encrypted (several new
17 commercially available operating systems provide for automatic encryption of data upon
18 shutdown of the computer).

19 c. Search Techniques: Searching the ESI for the items described in
20 Attachment B may require a range of data analysis techniques. In some cases, it is
21 possible for agents and analysts to conduct carefully targeted searches that can locate
22 evidence without requiring a time-consuming manual search through unrelated materials
23 that may be commingled with criminal evidence. In other cases, however, such
24 techniques may not yield the evidence described in the warrant, and law enforcement
25 personnel with appropriate expertise may need to conduct more extensive searches, such
26 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to
27 determine whether it falls within the scope of the warrant.
28

1 38. In this particular case, and in order to protect the third party privacy of
2 innocent individuals residing in the residence, the following are search techniques that
3 will be applied:

4 i. Device use and ownership will be determined through interviews, if
5 possible, and through the identification of user account(s), associated account names, and
6 logons associated with the device. Determination of whether a password is used to lock a
7 user's profile on the device(s) will assist in knowing who had access to the device or
8 whether the password prevented access.

9 ii. Use of hash value library searches.

10 iii. Use of keyword searches, i.e., utilizing key words that are known to be
11 associated with the sharing of child pornography.

12 iv. Identification of non-default programs that are commonly known to be used
13 for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent,
14 Ares, Shareaza, Gnutella, etc.

15 v. Looking for file names indicative of child pornography, such as, PTHC,
16 PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child
17 pornography.

18 vi. Viewing of image files and video files.

19 vii. As indicated above, the search will be limited to evidence of child
20 pornography and will not include looking for personal documents and files that are
21 unrelated to the crime.

22 39. These search techniques may not all be required or used in a particular
23 order for the identification of digital devices containing items set forth in Attachment B
24 to this Affidavit. However, these search techniques will be used systematically in an
25 effort to protect the privacy of third parties. Use of these tools will allow for the quick
26 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
27 and will also assist in the early exclusion of digital devices and/or files which do not fall
28

1 within the scope of items authorized to be seized pursuant to Attachment B to this
2 Affidavit.

3 40. In accordance with the information in this Affidavit, law enforcement
4 personnel will execute the search of digital devices seized pursuant to this warrant as
5 follows:

6 a. Upon securing the search site, the search team will conduct an initial
7 review of any digital devices/systems to determine whether the ESI contained therein can
8 be searched and/or duplicated on site in a reasonable amount of time and without
9 jeopardizing the ability to accurately preserve the data.

10 b. If, based on their training and experience, and the resources
11 available to them at the search site, the search team determines it is not practical to make
12 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
13 time and without jeopardizing the ability to accurately preserve the data, then the digital
14 devices will be seized and transported to an appropriate law enforcement laboratory for
15 review and to be forensically copied ("imaged"), as appropriate.

16 c. In order to examine the ESI in a forensically sound manner, law
17 enforcement personnel with appropriate expertise will produce a complete forensic
18 image, if possible and appropriate, of any digital device that is found to contain data or
19 items that fall within the scope of Attachment B of this Affidavit. In addition,
20 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
21 encrypted data to determine whether the data fall within the list of items to be seized
22 pursuant to the warrant. In order to search fully for the items identified in the warrant,
23 law enforcement personnel, which may include investigative agents, may then examine
24 all of the data contained in the forensic image/s and/or on the digital devices to view their
25 precise contents and determine whether the data fall within the list of items to be seized
26 pursuant to the warrant.

27 d. The search techniques that will be used will be only those
28 methodologies, techniques and protocols as may reasonably be expected to find, identify,

1 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
2 this Affidavit.

3 e. If, after conducting its examination, law enforcement personnel
4 determine that any digital device is an instrumentality of the criminal offenses referenced
5 above, the government may retain that device during the pendency of the case as
6 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
7 the chain of custody, and litigate the issue of forfeiture.

8 41. In order to search for ESI that falls within the list of items to be seized
9 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
10 search the following items (heretofore and hereinafter referred to as "digital devices"),
11 subject to the procedures set forth above:

12 a. Any digital device capable of being used to commit, further, or store
13 evidence of the offense(s) listed above;

14 b. Any digital device used to facilitate the transmission, creation,
15 display, encoding, or storage of data, including word processing equipment, modems,
16 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

17 c. Any magnetic, electronic, or optical storage device capable of
18 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
19 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
20 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

21 d. Any documentation, operating logs and reference manuals regarding
22 the operation of the digital device, or software;

23 e. Any applications, utility programs, compilers, interpreters, and other
24 software used to facilitate direct or indirect communication with the device hardware, or
25 ESI to be searched;

26 f. Any physical keys, encryption devices, dongles and similar physical
27 items that are necessary to gain access to the digital device, or ESI; and
28

1 g. Any passwords, password files, test keys, encryption codes or other
2 information necessary to access the digital device or ESI.
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

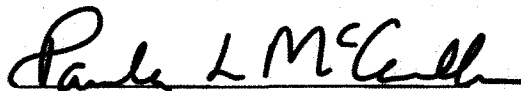
VI. CONCLUSION

42. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located at the SUBJECT PREMISES or on the SUBJECT PERSON as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. As shown by the aforementioned facts, I believe that the SUBJECT PERSON may be actively seeking sexually explicit relationships with minors and actively attempting to manufacture child pornography. I therefore request that the court issue a warrant authorizing a search of the location, vehicles, and person specified in Attachment A for the items more fully described in Attachment B.



Terry A. Getsch, Affiant
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing on this 1st day of October, 2018.



PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A

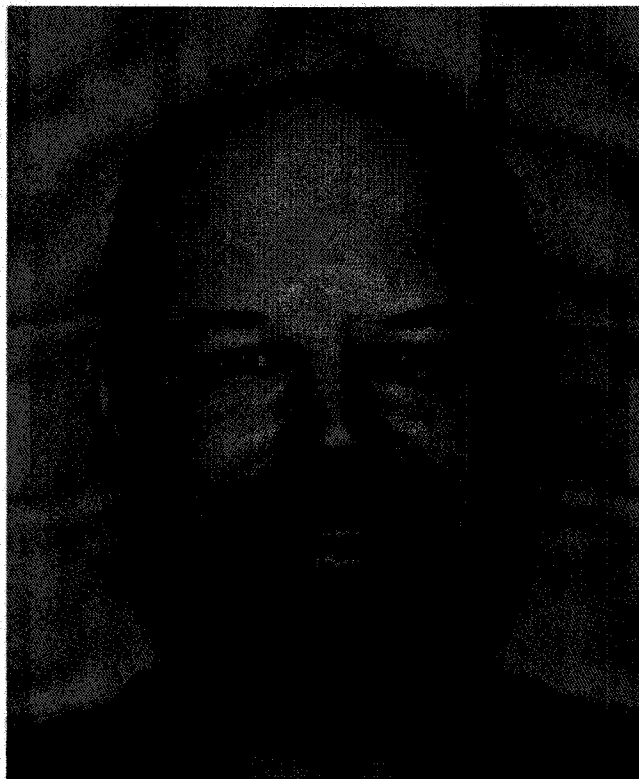
Description of Property to be Searched

1. The physical address of the SUBJECT PREMISES is 18737 Fisherman's Loop, Burlington, WA 98233. The SUBJECT PREMISES is the property at this address containing a single family, single story residence located in Skagit County, WA. The residence was previously identified by the Skagit County Tax assessor by the picture below:



The search is to include all rooms, persons, and vehicles on the SUBJECT PREMISES, as well as any garage/parking spaces or storage units/outbuildings located thereon and any digital device(s) found therein.

1 The SUBJECT PERSON is JAMES R. SIMS (DOB: XX/XX/1973), pictured
2 below:



ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence/records identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer, or evidences contact with minors;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

1 7. Digital devices and/or their components, which include, but are not limited
2 to:

3 a. Any digital devices and storage device capable of being used to
4 commit, further, or store evidence of the offense listed above;

5 b. Any digital devices used to facilitate the transmission, creation,
6 display, encoding or storage of data, including word processing equipment, modems,
7 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

8 c. Any magnetic, electronic, or optical storage device capable of
9 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
10 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
11 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

12 d. Any documentation, operating logs and reference manuals regarding
13 the operation of the digital device or software;

14 e. Any applications, utility programs, compilers, interpreters, and other
15 software used to facilitate direct or indirect communication with the computer hardware,
16 storage devices, or data to be searched;

17 f. Any physical keys, encryption devices, dongles and similar physical
18 items that are necessary to gain access to the computer equipment, storage devices or
19 data; and

20 g. Any passwords, password files, test keys, encryption codes or other
21 information necessary to access the computer equipment, storage devices or data;

22 8. Evidence of who used, owned or controlled any seized digital device(s) at
23 the time the things described in this warrant were created, edited, or deleted, such as logs,
24 registry entries, saved user names and passwords, documents, and browsing history;

25 9. Evidence of malware that would allow others to control any seized digital
26 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
27 as evidence of the presence or absence of security software designed to detect malware;
28 as well as evidence of the lack of such malware;

1 10. Evidence of the attachment to the digital device(s) of other storage devices
2 or similar containers for electronic evidence;

3 11. Evidence of counter-forensic programs (and associated data) that are
4 designed to eliminate data from a digital device;

5 12. Evidence of times the digital device(s) was used;

6 13. Any other ESI from the digital device(s) necessary to understand how the
7 digital device was used, the purpose of its use, who used it, and when.

8 14. Records and things evidencing the use of the IP addresses 172.92.195.206
9 (the SUBJECT IP ADDRESS) including:

10 a. Routers, modems, and network equipment used to connect
11 computers to the Internet;

12 b. Records of Internet Protocol (IP) addresses used;

13 c. Records of Internet activity, including firewall logs, caches, browser
14 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
15 entered into any Internet search engine, and records of user-typed web addresses.

16
17
18 **The seizure of digital devices and/or their components as set forth herein is**
19 **specifically authorized by this search warrant, not only to the extent that such**
20 **digital devices constitute instrumentalities of the criminal activity described above,**
21 **but also for the purpose of the conducting off-site examinations of their contents for**
22 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
23
24
25
26
27
28